



CATHOLIC EDUCATION OFFICE DIOCESE OF BATHURST

'With Jesus Christ as our inspiration and guide, we are called to provide high-quality Catholic education in the Diocese of Bathurst'

EMAIL AND INTERNET POLICY

1. Mission and Values

In partnership with the family, parish and community, our schools nurture a relationship with God in Christ Jesus, celebrate and share the Catholic faith, and educate to enable all to make a positive contribution to the world.

We are therefore committed to:

- a safe, inclusive and professional learning environment
- just and right relationships that recognise and respect the dignity of each individual
- the use of a variety of methods, technologies and techniques to enhance learning and teaching.

2. Purpose

- to inform staff of appropriate use of email and internet facilities in the workplace
- to ensure that procedures are in place to monitor the use of email and internet facilities in the workplace
- to ensure employees are aware of their rights and responsibilities under this policy.

This policy applies to all personnel employed by the Catholic Education Office as well as volunteers at the workplace.

3. Expectations

It is expected that all personnel to whom this policy applies will:

- abide by this policy
- take proper care of all diocesan ICT equipment
- respond appropriately to any report of misuse of diocesan email and internet facilities and bring any such report to the attention of their supervisor
- be informed of this policy annually by a supervisor.

4. Definitions

'Computer system' includes any workplace computer, any information held on these computers (whether or not the workplace owns that information), the local network, the wide area network, internet and email.

'Devices' means devices such as laptops, iPods and mobile phones, regardless of who they belong to, that are brought into the workplace or to workplace activities, or that are connected to any of the above mentioned networks or facilities.

"Email" is defined as all technologies and infrastructure used to transfer messages, including email, instant messaging and peer-to-peer file exchange. Email is a tool for business communications, which users have a responsibility to use in an efficient, effective, ethical and lawful manner. Email is inherently not secure, and sensitive or confidential material should not be sent through the electronic mail system unless it is encrypted.

"Internet" is defined as all technologies and infrastructure used to connect to and transfer data to and from the internet. The internet is an open network and is inherently not secure. Internet connectivity is provided for business and educational purposes, which users have a responsibility to use in an efficient, effective, ethical and lawful manner.

5. Guidelines

Property

All computer hardware, software, files/documents, email attachments and messages, email and Internet accounts maintained on the school and/or Bathurst Diocese computing systems are the sole property the Catholic Education Office Bathurst.

Monitoring

From time to time, the content and usage of email may be examined by the employer or by a third party on employer's behalf. This will include electronic communications that are sent both internally and externally.

The workplace computer network is a tool to be used primarily for business or educational purposes. Therefore there is a responsibility to use it in an appropriate, professional and lawful manner.

All messages on the workplace system will be treated as business or education related messages, which may be monitored. Accordingly, it should not be expected that any information or document transmitted or stored on the computer network will be private.

The workplace is able to monitor use of the internet, both during working hours and outside of those hours. This includes the internet sites and content that are accessed and the length of time spent using the internet.

Devices may be taken and access denied if it is believed that:

- there has been or may be a breach of a staff member's employment or engagement contract or a workplace policy
- there may be a threat of harm to a person or system security.

If unacceptable files and/or content is found those files/content must be reported to the principal or supervisor.

Permitted Use

Use of a workplace computer system, including email and Internet by staff is permitted and encouraged where such use is lawful, suitable for teaching, used for research or business purposes and supports the goals and objectives of the workplace.

Use of the CEO's or any of the school's domain names to conduct business other than official CEO or school business is prohibited.

The workplace may, as a matter of discretion, allow its computer system, including email and internet, to be used for other purposes, so long as this does not:

- contravene other parts of this policy
- adversely impact on performance of work duties

For example, as a matter of discretion, employees are permitted to use the internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum. However, excessive or inappropriate use of email or internet facilities for personal reasons may

result in limitation or removal of access to the workplace computer system. The employee should bear in mind that any use of the internet or email for personal purposes is still subject to the same terms and conditions as described in this policy.

Prohibited Use

The internet or email must not be used for the following purposes:

- to abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other)
- to send or receive obscene or pornographic material
- to harm the reputation of the workplace or to cause embarrassment to the workplace
- to spam or mass mail, or to send or receive chain mail
- to infringe the copyright or other intellectual property rights of another person
- to perform any other unlawful or inappropriate act
- to download video files or downstream from the internet
- to download excessive quantities of data, other than in the ordinary course of performing duties for the workplace
- to game, wage or bet
- to perform any activity using an anonymous or misleading identity
- to access the internet using another person's name or account
- to gain, or attempt to gain, unauthorised access to any website or to any person's servers, networks or databases
- to compromise the workplace computer system
- to disclose confidential or sensitive information
- to alter or copy a message or attachment belonging to another user without the permission of the originator
- to subscribe to list servers and distribution lists unless they are directly related to the workplace role
- to conduct business other than official CEO or school business by using domain names of CEO or school
- to conduct any other illegal activity.

Comments that are not appropriate in the workplace will also be inappropriate when sent by email.

Email messages can easily be misconstrued. Words and attached documents should therefore be carefully chosen and expressed in a clear, professional manner.

An employee who receives inappropriate material by email should report it to the principal or supervisor immediately and not forward it to anyone else. It would be appropriate for the principal or supervisor to discourage the sender from sending further material of that nature.

Software (licensed, shareware, freeware, evaluation or otherwise) including system, application or data files, may only be downloaded in accordance with the instructions of the workplace.

Possession of child pornography is a criminal offence and grounds for dismissal.

Intellectual Property

The CEO is the owner of copyright in all email messages created by staff as part of their work for the Diocese. Staff must not infringe the intellectual property rights of other people.

Material staff want to distribute or copy may be subject to copyright. This includes files staff may wish to download, such as images, cartoons and music. Copyright material owned by other people must not be distributed or copied without the permission of the copyright owner, unless authorized by the Copyright Act as a fair dealing, under the educational statutory licence or another exception.

Privacy

In the course of carrying out duties on behalf of the workplace, personal information relating to others, including, but not limited to, students, clients, colleagues, contractors, parents and suppliers may be accessed. Internet or email should not be used to disclose personal information except in accordance with the workplace privacy policy or with proper authorisation. The Privacy Act requires staff to take reasonable steps to protect personal information from misuse and unauthorised access. It is therefore critical that staff take responsibility for the security of their personal computer and not allow it to be used by an unauthorised party, which specifically includes anyone who is not an employee of the CEO.

In order to comply with obligations under the Privacy Act, staff are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of email addresses will impinge upon the privacy of the recipients.

All emails should contain the standard disclosure message:

The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please advise immediately by telephone (reverse charges) and then delete/destroy the email and any printed copies. Thank You.

Security

Employees will be assigned a username and will be required to select a password to use the workplace electronic communications facilities. These details should not be disclosed to anyone else and steps should be taken to keep these details secure.

Employees are responsible for their computer work stations and are encouraged to either lock their screen or log-out when they leave their desk. This will avoid others gaining unauthorised access to personal or confidential information within the workplace.

All external files and attachments must be virus checked using scanning software before they are accessed. The downloading of infected information from the internet is potentially fatal to the workplace computer network.

Breach of this Policy

Proven breaches of this policy can result in, but is not limited to, any one or more of the following:

- Disciplinary action
- Dismissal
- Notification to an external agency
- Criminal charges

These breaches should be reported to principal or supervisor.

Contractors who engage in unacceptable behaviour may have their contract or engagement with the school terminated or not renewed.

General

The terms and recommended conduct described in this policy are not intended to be exhaustive, nor do they anticipate every possible use of the workplace email and internet facilities. Employees should act with caution and take into account the underlying principles intended by this policy. If an employee feels unsure of the appropriate action relating to use of email or the internet, he or she should speak to a supervisor. Use of the workplace computer network that is inappropriate or inconsistent with this policy may result in disciplinary action, including termination of employment.

6. Legislative Framework

1. Copyright Act 1977
2. Anti-Discrimination Act 1977
3. Racial Discrimination Act 1975
4. Disability Discrimination Act 1992
5. Sex Discrimination Act 1984
6. Occupational Health and Safety Act 2000
7. Workplace Relations Act 1996 (Commonwealth)

7. Related Policies and Guidelines

1. Workplace Grievance Policy Catholic Education Office Bathurst 2009
2. Staff Discipline Policy Catholic Education Office Bathurst 2009
3. Occupational Health and Safety Policy Catholic Education Office Bathurst 2009
4. Guidelines for the Management of Complaints Catholic Education Office Bathurst 2009
5. Procedures for Managing Cyberbullying Catholic Education Office Bathurst 2008
6. Code of Conduct For Employees Catholic Education Office Bathurst 2009
7. Discrimination, Harassment and Bullying Policy Catholic Education Office Bathurst 2009

8. Policy Administration

This policy has been ratified by the Executive Director of Schools and will be reviewed periodically, or in the event of any information or incident that indicates the need for a review, or following relevant legislative or organisational change.

It is the responsibility of anyone accessing this document to ensure that the current version is downloaded from the CEO website.

Date of Implementation	September 2009
Date of Last Review	N/A
Date for Next Review	September 2012